IACR 2006 Election DRAFT BALLOT

DRAFT

1. POLICY CHANGE

Please choose between the following two IACR policy options to take effect as of July 1, 2007.

↳ **Vote** for at most one (1) of the following policy options by marking ☑ beside your response.

- □ Submissions to all IACR conferences (Asiacrypt, Crypto, and Eurocrypt) should normally be anonymous to program committee members throughout the reviewing process. Authorship should only be disclosed by the program chair in rare instances involving conflicts or other special circumstances.
- □ The policy on anonymity of submissions should be left to the discretion of the program chair of each IACR conference.

2. THREE DIRECTORS

Election is being held for three (3) directors for the IACR Board of Directors. These directors will serve a three-year term from 1 January 2007.

Names are presented in a shuffled order. Candidates' statements (in the same order) may be found on the following page.

↳ **Vote** for up to three (3) of the candidates by marking ☑ beside your response.

Director (vote for no more than three):

- □ Josh Benaloh
- □ Arjen Lenstra
- □ Anna Lysyanskaya
- □ Tom Berson
- □ Jovan Golic
- □ Lars Knudsen
- □ David Naccache
- □ Serge Vaudenay

DRAFT

3. RETURN YOUR BALLOT

↳ **Seal your completed ballot in the small envelope** marked “Ballot”. Do not write anything on the small envelope. This will preserve anonymity of your vote.

↳ **Seal the small envelope in the large envelope** with the printed address of the Returning Officer (James Hughes).

↳ **Print your name and place your signature on the large envelope.** This is very important. It is used to authenticate your vote.

↳ **Send the large envelope to the returning officer.** Only ballots received by midnight (EST) on 15 November 2006 will be counted. You may need to use Air Mail. Be sure to attach sufficient postage.

DRAFT

CANDIDATES' STATEMENTS

Josh Benaloh: I have served on the IACR Board for the past eight years -- the first six as IACR secretary and the past two as General Chair of Crypto 2006. I seek the opportunity to continue serving in an at-large position. Please see http://research.microsoft.com/crypto/benaloh/iacr.html for a more complete statement. Thank you.

Longer statement: http://research.microsoft.com/crypto/benaloh/iacr.html

Home page: http://research.microsoft.com/crypto/benaloh

Arjen Lenstra: Continue support of scientific status and relevance of IACR activities, keep working on more affordable registration fees.

Anna Lysyanskaya: The IACR is my home research community, and I'd like to give back. My priorities are:

- High quality and effective dissemination
- Tutorials and mentoring
- Dialogue with related research communities, industry, standards and funding agencies

I promise to approach all issues with enthusiasm and an open mind.

Longer statement: http://www.cs.brown.edu/~anna/iacr-election.html

Home page: http://www.cs.brown.edu/~anna

Tom Berson: I have served IACR since 1983 as Secretary, Treasurer, President, and Director. During that time we created conferences, cryptologic literature, and community. Our present challenges include maintaining balance and tolerance in the evolving community. I know where we have been; I know where we are going. Please vote for me.

Longer statement: http://www.anagram.com/vote

Home page: http://www.anagram.com/berson

DRAFT

Jovan Golić: Many of you know me for research in cryptography in the last two decades. Due to increasing numbers of submissions, the quality of the reviewing process of IACR-sponsored conferences/workshops has been deteriorating seriously. My main objective is to improve the situation and make the process fair, accountable, and transparent.

Lars R. Knudsen: I want more papers accepted at Crypto, Eurocrypt and Asiacrypt. Skip the free Tuesday afternoon, extend the conferences until Friday noon, rump session Thursday evening. I propose for next by-laws update to have the rule that a director can serve for at most three periods (not counting Officers positions).

Longer statement: http://www2.mat.dtu.dk/people/Lars.R.Knudsen/iacr.html

Home page: http://www.ramkilde.com/iacr.html

David Naccache:

```
d7e098bf 4a3be052 71e01c71 7933bf0c b7fde090 ce71d63b fd0ce0de
2b0ce00c 98bf0ce0 715ae01c 71b75279 e033a7e0 de3bed0c e00c71e0
983b1490 e0712bce e0bfeded 71fdb7bf 0cb77152 e01c3b4a 3b147190
e0bf521c e0ce2b52 e0ed3371 710c9814 a792e02c 98bf52f5 ede05a71
cee04a71 0cb75279 e05a71ce e0333b92
```

Home page: http://www.di.ens.fr/DavidNaccache.html

Serge Vaudenay: I would like to work on

- Maintaining high quality standards in conference programs. I will suggest implementing quality controls in program committees.
- Keeping the cryptography area as broad as possible.
- Promoting academic careers in the field of cryptography, notably by working on the new best paper award and fellowship tradition.

Home page: http://lasecwww.epfl.ch/~vaudenay